

Università degli Studi di Siena



Regolamento per l'utilizzo di sistemi di videosorveglianza nei locali del palazzo del rettorato dell'Università degli Studi di Siena

(Emanato con D.R. n. 320 del 6 Dicembre 2007, pubblicato nel B.U. n. 72)

Sommario

| | | |
|-----------|--|---|
| Art. 1 - | Ambito di applicazione e finalità..... | 3 |
| Art. 2 - | Definizioni | 3 |
| Art. 3 - | Principi generali..... | 4 |
| Art. 4 - | Conservazione e cancellazione dei dati | 4 |
| Art. 5 - | Modalità di raccolta dati personali | 4 |
| Art. 6 - | Comunicazione dati..... | 5 |
| Art. 7 - | Responsabilità, gestione operativa, sicurezza dati..... | 5 |
| Art. 8 - | Informativa agli utenti | 5 |
| Art. 9 - | Diritti dell'interessato | 5 |
| Art. 10 - | Informativa sindacale | 5 |
| Art. 11 - | Applicabilità della disciplina del regolamento ad altri plessi dell'Università degli Studi di Siena..... | 6 |
| Art. 12 - | Norma di rinvio..... | 6 |
| Art. 13 - | Entrata in vigore..... | 6 |

Art. 1 - *Ambito di applicazione e finalità*

1. Il presente regolamento disciplina il trattamento di dati personali realizzato mediante impianti di videosorveglianza collocati all'interno dei locali del rettorato dell'Università degli Studi di Siena. La registrazione delle immagini avviene con videocamere a immagine fissa installate al fine di tutelare il patrimonio universitario e allo scopo di prevenire atti vandalici, ovvero per indagini di polizia giudiziaria.
2. Il presente regolamento garantisce che il trattamento dei dati personali effettuato mediante l'attivazione di impianto di videosorveglianza nei locali interni del Palazzo del rettorato dell'Università degli Studi di Siena, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, garantendo altresì i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento.
3. Le immagini ed i dati raccolti non possono essere utilizzati per finalità diverse rispetto a quelle stabilite nel presente regolamento e nell'apposito documento di cui al successivo art. 3 e non possono essere diffusi o comunicati a terzi, salvo quanto di seguito disposto.
4. L'Università degli Studi di Siena garantisce che le immagini non siano in alcun modo impiegate come strumento di sorveglianza a distanza dei docenti, del personale tecnico ed amministrativo, degli studenti e degli altri utenti dell'Università, sia con riguardo alle funzioni ed attività da essi esercitate all'interno dell'Ateneo, sia con riferimento alle rispettive abitudini personali.
5. I programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art. 2 - *Definizioni*

1. Ai fini del presente regolamento si intende:
 - a. per "**banca dati**", il complesso di dati personali formatosi presso gli specifici e appositi locali della portineria del rettorato, e trattato esclusivamente mediante riprese televisive, che in relazione ai luoghi di installazione delle videocamere riguardano prevalentemente i soggetti che transitano nell'area interessata;
 - b. per "**trattamento**", tutte le operazioni o complesso di operazioni, svolte con l'ausilio dei mezzi elettronici o comunque automatizzati concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, l'eventuale diffusione, la cancellazione e la distruzione di dati;
 - c. per "**dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, e rilevati con trattamenti di suoni ed immagini effettuati attraverso l'impianto di videosorveglianza;
 - d. per "**misure minime**": il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che garantiscono il livello minimo di protezione previsto dalle norme;
 - e. per "**titolare**", l'Università degli Studi di Siena;
 - f. per "**responsabile**", il Dirigente dell'Area Servizi Generali dell'Università degli Studi di Siena;
 - g. per "**incaricato**" la persona fisica autorizzata dal Responsabile a compiere operazioni di trattamento dal titolare o dal responsabile;
 - h. per "**interessato**", la persona fisica, la persona giuridica, l'ente o associazione cui si riferiscono i dati personali;
 - i. per "**comunicazione**", il dare conoscenza dei dati personali a soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
 - j. per "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- k. per "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- l. per "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
- m. per "**Codice**", il D.lgs. 30.06.2003 n. 196 in materia di protezione dei dati personali;
- n. per "**Garante**", l'Autorità Garante per la protezione dei dati personali;
- o. per "**Provvedimento Generale**" il Provvedimento del Garante del 29.04.2004.

Art. 3 - *Principi generali*

1. Principio di liceità

Il trattamento dei dati attraverso sistemi di videosorveglianza nei locali del rettorato dell'Università degli Studi di Siena è fondato sui presupposti di liceità che il Codice prevede espressamente per gli organi pubblici (svolgimento di funzioni istituzionali: artt. 18-22¹). In particolare, possono essere attivati sistemi di videosorveglianza solo in quanto siano strumentali allo svolgimento delle funzioni istituzionali e il relativo trattamento deve avvenire nel rispetto della disciplina in materia di protezione dei dati e di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi².

2. Principio di necessità

Nell'installazione di un sistema di videosorveglianza nei locali del rettorato dell'Università degli Studi di Siena è escluso ogni uso superfluo e sono evitati eccessi e ridondanze³.

3. Principio di proporzionalità

L'installazione di impianti di videosorveglianza nei locali del rettorato dell'Università degli Studi di Siena è fondato su una ponderata valutazione circa l'insufficienza e l'inattuabilità di altre misure, nel rispetto del principio di proporzionalità sia nella scelta se e quali apparecchiature di ripresa installare, sia nelle varie fasi del trattamento⁴.

4. Principio di finalità

Gli scopi perseguiti con l'installazione di impianti di videosorveglianza sono determinati, espliciti e legittimi⁵. A tal fine le ragioni che hanno determinato l'installazione di impianti di videosorveglianza nei locali del rettorato dell'Università degli Studi di Siena sono esplicitate in apposito atto (All. 1).

Art. 4 - *Conservazione e cancellazione dei dati*

1. Tenuto conto del fatto che il sistema di videosorveglianza è programmato in modo da prevedere, dopo 24 ore dalla registrazione, la cancellazione automatica da ogni supporto, mediante sovraregistrazione e con modalità che rendono non riutilizzabili i dati cancellati, le immagini contenute nella videoregistrazione sono conservate, ordinariamente, per un massimo di 24 ore dalla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici e servizi, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

2. In caso di cessazione di un trattamento per qualsiasi causa, i dati personali sono comunque distrutti.

Art. 5 - *Modalità di raccolta dati personali*

1. I dati personali sono ripresi attraverso le telecamere ad immagine fissa dell'impianto di videosorveglianza installato nei locali del rettorato e dichiarato dall'installatore conforme alle misure minime ed alle norme previste dal Codice. A tal proposito il responsabile del trattamento deve ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle regole in materia.

2. La dislocazione delle telecamere risulta dall'allegato 2) al presente regolamento modificabile dal responsabile del trattamento dei dati che ne informa senza indugio il Titolare del trattamento.

3. I soggetti incaricati al trattamento, autorizzati ad utilizzare gli impianti e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni, sono designati tramite atto scritto dal

responsabile del trattamento (All. 3) e sono tenuti a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto.

4. Il responsabile del trattamento informerà per iscritto le persone incaricate al trattamento sulle loro responsabilità relative al trattamento e alla conservazione dei dati, alla loro protezione da eventi dannosi e agli altri obblighi di legge. Tali istruzioni dovranno essere aggiornate in caso di modifiche tecniche e normative.

Art. 6 - *Comunicazione dati*

1. La comunicazione dei dati personali raccolti presso il rettorato è consentita nei limiti di legge.
2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal titolare o dal responsabile.

Art. 7 - *Responsabilità, gestione operativa, sicurezza dati*

1. Il responsabile del trattamento di cui all'art. 2, comma 1, lett. f) svolge i seguenti compiti:
 - a. nomina con atto scritto gli incaricati al trattamento;
 - b. cura i rapporti tra l'Università ed il soggetto incaricato del trattamento dei dati, coordinandone l'attività;
 - c. vigila sulla conservazione delle immagini e sulla loro distruzione al termine del periodo previsto per la conservazione delle stesse;
 - d. ha la responsabilità del procedimento volto all'esercizio del diritto di accesso ai dati da parte dell'interessato e/o delle autorità competenti.
2. L'accesso alla sala di controllo posta nei locali della portineria del rettorato è consentito al responsabile, agli incaricati del trattamento, al personale di pubblica sicurezza o di polizia giudiziaria, nonché al personale addetto alla manutenzione degli impianti ed alla pulizia dei locali.
3. Il responsabile della gestione e del trattamento impartisce idonee istruzioni tecniche per evitare assunzioni o rilevamento di dati da parte di persone non autorizzate a tali scopi.

Art. 8 - *Informativa agli utenti*

1. In ottemperanza a quanto disposto dall'art. 13 del Codice⁶ e successive modifiche e integrazioni, in prossimità delle postazioni in cui sono state installate le telecamere è affissa adeguata segnaletica permanente contenente la comunicazione e l'avvertimento al pubblico (utenti e intera comunità accademica) delle finalità e delle modalità di ripresa in modo da renderle conoscibili a tutti (All. 4 e All. 5).

Art. 9 - *Diritti dell'interessato*

1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, potrà:
 - a. ottenere la conferma dell'esistenza di trattamenti di dati che possono riguardarlo;
 - b. essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;
 - c. opporsi, motivatamente, in tutto o in parte al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.
2. Le istanze di cui al presente articolo devono essere trasmesse al titolare (Università degli Studi di Siena) o al responsabile del trattamento (dirigente dell'Area Servizi Generali) in forma scritta.

Art. 10 - *Informativa sindacale*

1. Ai sensi dell'art. 4, legge n. 300/1970 ed in applicazione del divieto di utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività lavorativa, nel caso in cui dall'installazione di impianti di videosorveglianza derivi, direttamente o indirettamente, la

possibilità di controllo a distanza dell'attività delle/dei lavoratrici/lavoratori, gli impianti stessi possono essere installati soltanto previo accordo con le rappresentanze sindacali unitarie di Ateneo⁷. A tal fine ogniqualvolta si verifichi tale ipotesi, il responsabile della struttura interessata deve darne comunicazione scritta, preliminare all'installazione, al Rettore.

Art. 11 - *Applicabilità della disciplina del regolamento ad altri plessi dell'Università degli Studi di Siena*

1. La disciplina del trattamento dei dati tramite sistemi di videosorveglianza contenuta nel presente regolamento verrà resa pubblica e comunicata a tutti i responsabili delle varie strutture dell'Ateneo diverse da quelle di cui art.2, comma 1, lett. a) che, nel caso di installazione di impianti di videosorveglianza, sono tenuti ad adeguare la regolamentazione dell'installazione di impianti presso i plessi e i locali di propria pertinenza ai principi contenuti nel presente regolamento.

2. A tal fine ogni struttura dotata di autonomia regolamentare all'interno della quale si intenda installare un impianto di videosorveglianza, dovrà provvedere ad adottare il regolamento di disciplina sull'utilizzo degli impianti di videosorveglianza con deliberazione del proprio Consiglio, provvedendo alla nomina del responsabile del trattamento e dei vari incaricati, ed informando successivamente il dirigente dell'Area Servizi Generali, allegando il regolamento di disciplina e gli atti di nomina.

3. Nei casi e per le finalità di cui al precedente articolo 11, ogniqualvolta dall'installazione di impianti di videosorveglianza derivi, direttamente o indirettamente, la possibilità di controllo a distanza dell'attività delle/dei lavoratrici/lavoratori, i responsabili della struttura interessata devono darne comunicazione scritta, preliminare all'installazione, al Rettore.

Art. 12 - *Norma di rinvio*

1. Per quanto non previsto dal presente regolamento, si applicano le disposizioni previste dal D.lgs. 30 giugno 2003 n. 196, le altre disposizioni legislative comunque attinenti e le disposizioni contenute nei Provvedimenti emessi in materia dal Garante e dalla Funzione Pubblica e allegati al presente regolamento.

Art. 13 - *Entrata in vigore*

1. Il presente regolamento entra in vigore il giorno successivo a quello della sua emanazione ed è pubblicato sul Bollettino Ufficiale dell'Ateneo e sul sito web dell'Università.

Allegato n. 1

Documento sulle ragioni della videosorveglianza

L'Università degli Studi di Siena, in persona del Rettore pro-tempore, Prof. Silvano Focardi

premesse:

- che svolge attività di.....;
- che l'attività è svolta nei seguenti locali:
- Edificio del Rettorato
- che negli stessi, oltre alle attrezzature per l'esercizio dell'attività lavorativa vi sono:

-
-
- che i locali sono situati in zona facilmente accessibile;
 - che pur avendo adottato sistemi di tutela dei locali è necessario un sistema di sorveglianza mediante videocamere, che possa garantire un maggiore e più tempestivo controllo degli accessi, in particolare dei seguenti locali

durante i periodi in cui si svolge normale attività lavorativa;

- che tale sistema è stato individuato mediante il posizionamento di n. _____ videocamere che effettua registrazione di immagini;
- che le immagini verranno trattate nel rispetto delle prescrizioni di cui al provvedimento del Garante per la tutela dei dati personali del 29 aprile 2004

Tutto ciò premesso

certifica quanto sopra ai fini di quanto stabilito dal provvedimento citato nella sua qualità di **Titolare del trattamento dei dati personali**

_____, li _____

Il Titolare del trattamento
Università degli Studi di Siena
Il Rettore

Allegato n. 2

Elenco delle telecamere

Allegato n. 3

Atto di nomina dell'incaricato (lettera di incarico) alla videosorveglianza ai sensi e per gli effetti del D.Lgs. 30 giugno 2003, n. 196

Egr. Sig. / Gent. Sig.ra.....

Oggetto: utilizzazione impianto di videosorveglianza

Il locali del palazzo del rettorato dell'Università degli Studi di Siena sono forniti di impianto di videosorveglianza a mezzo telecamera fissa, per il controllo dell'accesso ai seguenti locali o aree:

L'apparecchiatura di controllo è installata nell'apposito locale situato:

In relazione a quanto disposto dal Garante per la tutela dei dati personali (provvedimento del 29.4.2004) Le conferisco la facoltà di utilizzare tale sistema di videosorveglianza negli orari di lavoro.

Le ricordo che il sistema in questione è utilizzato per il seguente scopo _____ (ad esempio garantire la sicurezza degli accessi).

Le immagini sono fisse, senza ingrandimenti o dettagli.

Siena, li _____

Il Responsabile del trattamento

L'incaricato alla videosorveglianza



N.B.: Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

Allegato n. 5

Informativa sulla videosorveglianza

IL PRESENTE LOCALE PER RAGIONI DI SICUREZZA E' SORVEGLIATO DA SISTEMA DI VIDEOSORVEGLIANZA FISSA A MEZZO TELECAMERA..

LE IMMAGINI VENGONO REGISTRATE/RILEVATE NEL SEGUENTE MODO¹:

L'USO DEI SISTEMI DI VIDEOSORVEGLIANZA E IL TRATTAMENTO DELLE IMMAGINI E' DEMANDATO ESCLUSIVAMENTE AI SOGGETTI SPECIFICAMENTE INCARICATI DALL'UNIVERSITA' DEGLI STUDI DI SIENA, CON ATTO SCRITTO.

IL CONFERIMENTO DEI DATI E DELLE IMMAGINI NON E' OBBLIGATORIO, MA IL DIVIETO DI RIPRESA POTRA' COMPORTARE L'IMPOSSIBILITA' DI AUTORIZZARE L'ACCESSO AI LUOGHI OGGETTO DI VIDEOSORVEGLIANZA.

RESTANO FERME LE ESIGENZE DI CONTROLLO E SICUREZZA ANCHE NELL'AMBITO DI INDAGINI INVESTIGATIVE.

I SOGGETTI INTERESSATI RIPRESI DALLE VIDEOCAMERE POSSONO ESERCITARE I DIRITTI DI CUI ALL'ART. 7 DEL D. LGS. n. 196/03.

TITOLARE DEL TRATTAMENTO DEI DATI E' L'UNIVERSITA' DEGLI STUDI DI SIENA.
RESPONSABILE DEL TRATTAMENTO DEI DATI E' IL DIRIGENTE DELL'AREA SERVIZI GENERALI

¹ Es: su nastro magnetico....

¹ D. Lgs. 30.06.2003, n. 196

Art. 18. Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici.

1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.
2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.
3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.
4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.
5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione.

Art. 19. Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari.

1. Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.
2. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.
3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Art. 20. Principi applicabili al trattamento di dati sensibili.

1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.
2. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo.
3. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.
4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente.

Art. 21. Principi applicabili al trattamento di dati giudiziari.

1. Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.
2. Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari.

Art. 22. Principi applicabili al trattamento di dati sensibili e giudiziari.

1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.
2. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.
3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.
4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.
5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.
6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

10. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.

11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.

12. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.

² Cfr. ***Provvedimento a carattere generale del Garante della protezione dei dati personali del 29 aprile 2004***

“(…) Vanno richiamate al riguardo le vigenti norme dell’ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell’immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela (toilette, stanze d’albergo, cabine, spogliatoi, ecc.). Vanno tenute presenti, inoltre, le norme riguardanti la tutela dei lavoratori, con particolare riferimento alla legge 300/1970 (Statuto dei lavoratori).

Specifici limiti possono derivare da altre speciali disposizioni di legge o di regolamento che prevedono o ipotizzano la possibilità di installare apparecchiature di ripresa locale, aerea o satellitare (d.l. 24 febbraio 2003, n. 28, convertito, con modificazioni, dalla legge 24 aprile 2003, n. 88), disposizioni che, quando sono trattati dati relativi a persone identificate o identificabili, vanno applicate nel rispetto dei principi affermati dal Codice, in tema per esempio di sicurezza presso stadi e impianti sportivi, oppure musei, biblioteche statali e archivi di Stato (d.l. 14 novembre 1992, n. 433, convertito, con modificazioni, dalla legge 14 gennaio 1993, n. 4) e, ancora, relativi a impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali (d.lg. 4 febbraio 2000, n. 45).

Appare inoltre evidente la necessità del rispetto delle norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni”.

³ Cfr. ***Provvedimento a carattere generale del Garante della protezione dei dati personali del 29 aprile 2004***

“(…) Ciascun sistema informativo e il relativo programma informatico vanno conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., programma configurato in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini). Il software va configurato anche in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati.

Se non è osservato il principio di necessità riguardante le installazioni delle apparecchiature e l’attività di videosorveglianza non sono lecite (artt. 3 e 11, comma 1, lett. a), del Codice)”.

⁴ Cfr. art. 11, comma 1, lett. d) del Codice.

⁵ Cfr. art. 11, comma 1, lett. d) del Codice.

⁶ **Art. 13. Informativa.**

1. L’interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

- a) le finalità e le modalità del trattamento cui sono destinati i dati;
- b) la natura obbligatoria o facoltativa del conferimento dei dati;
- c) le conseguenze di un eventuale rifiuto di rispondere;
- d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l’ambito di diffusione dei dati medesimi;
- e) i diritti di cui all’articolo 7;
- f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell’articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l’elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all’interessato in caso di esercizio dei diritti di cui all’articolo 7, è indicato tale responsabile.

2. L’informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto

l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

5. La disposizione di cui al comma 4 non si applica quando:

- a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
- c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiara manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

⁷ ***Cass. Civ. Sez. Lav., sent. n. 4746 del 03-04-2002***

“Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 della legge n. 300 del 1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aule riservate o, come nella specie, gli apparecchi di rilevazione di telefonate ingiustificate”.